U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

14.3.5[1] INSTRUMENTATION AND CONTROLS (Tier 1)

REVIEW RESPONSIBILITIES

Primary - Instrumentation and Controls Branch (HICB)

Secondary - None

I. AREAS OF REVIEW

The information to be reviewed is the Tier 1 information and the inspections, tests, analyses, and acceptance criteria (ITAAC) for instrumentation and control (I&C) systems proposed by the applicant. This review should be coordinated with the review of the applicant's I&C systems design as described in Chapter 7 of the SRP. The reviewer's primary responsibilities include a review of Tier 1 for I&C systems involving reactor protection and control, engineered safety features actuation, other miscellaneous I&C systems, additional material in Tier 1 related to application of digital computers in I&C systems, and selected interface requirements related to I&C issues. HICB has secondary review responsibilities for ESF systems, reactivity control systems, and other systems using I&C equipment.

Review Interfaces

SRP Section 14.3 provides general guidance on review interfaces. HICB performs related reviews and coordination activities, as requested by other branches, for issues in Tier 1 related to

I&C systems. In addition, HICB will coordinate other branches' evaluations that interface with the overall review of the systems as follows:

1. The Reactor Systems Branch (SRXB) determines the acceptability of Tier 1 information regarding reactor and core cooling systems design features that prevent and mitigate design basis accidents in SRP Section 14.3.4.

2. The Electrical Engineering Branch (EELB) determines the acceptability of Tier 1 information regarding electrical issues in SRP Section 14.3.6.

Standard ITAAC entries for several attributes of I&C systems are listed in Appendix D to this SRP section. HICB is responsible for consistent use of the standard ITAAC in Tier 1 for electrical isolation and physical separation (independence) as it pertains to I&C issues. Guidance regarding its use should be provided to other branches as appropriate.

II. ACCEPTANCE CRITERIA

The acceptance criteria for ITAAC are based on meeting 10 CFR 52.97(b)(1), which sets forth the comprehensive requirements for ITAAC. For design certification reviews, the scope of ITAAC is limited to the scope of the certified design as required by 10 CFR 52.47(b).

1. For I&C systems, acceptability is based on meeting the relevant requirements of the following regulations:

   10 CFR 50.55a(h), "Criteria for Protection Systems for Nuclear Generating Stations," and IEEE Standard 279-1971, as it pertains to safety-related protection systems requirements.

   GDC 1, as it pertains to quality standards and records requirements

   GDC 2, as it pertains to protection against natural phenomenon

   GDC 4, as it pertains to environmental and dynamic effects

   GDC 13, as it pertains to instrumentation and control requirements

   GDC 19, as it pertains to control room requirements

   GDC 20, as it pertains to protection system design requirements

   GDC 21, as it pertains to protection system reliability and testability requirements

   GDC 22, as it pertains to protection system independence requirements

   GDC 23, as it pertains to protection system failure modes requirements

   GDC 24, as it pertains to separation of protection systems from control systems

GDC 25, as it pertains to protection system requirements for reactivity control malfunctions

GDC 29, as it pertains to protection against anticipated operational occurrences requirements

To meet the above regulations, the appropriate Tier 1 and ITAAC entries should address the following design issues:

(1) General functional requirements for the system

(2) Hardware and software architecture

(3) Single failure criterion

(4) Quality of components and modules (hardware, software, and firmware)

(5) Equipment qualification (mild and harsh environments)

(6) Channel integrity and channel independence

(7) Classification of equipment

(8) Isolation devices (electrical and data)

(9) Single random failure

(10) System inputs

(11) Capability for sensor checks, tests and calibration

(12) Channel bypasses, operating bypasses, indication of bypasses, and access to means for bypassing

(13) Completion of protective action once initiated

(14) Manual initiation

(15) Information read-out

(16) Identification

Tier 1 should be reviewed for adequacy of both safety-related and non-safety-related systems of the design. The I&C design described in SSAR and Tier 1 may be to the level of control functional blocks. The block concept is useful for developing the system control interface diagrams that are needed for depicting the configuration of the I&C

system architecture. Criteria from the SRP applicable to those systems should be used in the review.

2. For the microprocessor and digital control technology aspects of the I&C system design, applicants may provide incomplete design information in DCD Tier 2. This is because the digital computer-based I&C systems are a rapidly changing technology, and therefore it may not be appropriate for applicants to "lock in" the design for the time from design certification until the actual construction of the facility, when it could be obsolete. The staff allows the applicant to provide the processes and design acceptance criteria (DAC) by which the details of the design would be developed, designed, and evaluated. Detailed supporting information is in DCD Tier 2 Chapters 7 and 14.3. In lieu of having a completed I&C design for review, the reviewer must base the safety determination on an acceptable process for the design of the I&C systems, and related design acceptance criteria (DAC). The DAC are described further in Appendix A of this SRP Chapter.

   The issues discussed in the DAC should include the design of the safety system and plant protection system controls, development and qualification processes for I&C hardware and software, and design features that provide I&C system diversity as protection against common mode failures and address defense-in-depth considerations. These issues and their relationships to other systems of the design should be described in Tier 1. Figures may be used for this at a block diagram level.

   The description of the logic and control should address automatic decision-making and trip logic functions, and manual initiation functions associated with the safety actions of the safety-related systems. Instrumentation and control equipment may include microprocessor-based, software-controlled signal processors that perform signal conditioning, setpoint comparison, trip logic, system initiation and reset, self-test, calibration, and bypass functions. The signal processors associated with a particular safety-related system are usually considered to be an integral part of that system. Some I&C systems may be shared (such as a multiplexor system) and may be addressed in SSAR as a separate system. The safety determination and, therefore, the requirements that a separately described I&C system must meet will be determined by the safety significance of the systems that it is supporting.

   Tier 1 should address the development and qualification processes for I&C equipment. The discussion should include (1) design processes and acceptance criteria to be used for safety-related systems using programmable microprocessor-based control equipment, (2) a program to assess and mitigate the effects of electromagnetic interference on I&C equipment, (3) a program to establish setpoints for safety-related instrument channels, and (4) a program to qualify safety-related I&C equipment for in-service environmental conditions.

   Tier 1 should address the hardware and software development process to be used in the design, testing, and installation of I&C equipment. Tier 1 includes the description of the design process to be followed for hardware and software development, design commitments, the inspections, tests, and analysis to be performed to verify that the design is consistent with the commitments, and the appropriate acceptance criteria

against which the design will be judged. This ITAAC describes attributes of the process to be used to develop the I&C systems as well as attributes of the final product. The ITAAC for software and hardware verifies the applicant's proposed design stages within the overall design process. The various stages are described in more detail in DCD Tier 2. An example of various design stages is given below.

(1) Planning
(2) Design definition
(3) Software design
(4) Software coding
(5) Integration
(6) Validation
(7) Change control

Tier 1 and DCD Tier 2 contain criteria which describe the method to develop plans and procedures that will guide the design process throughout the lifecycle stages. The ITAAC provides the acceptance criteria for verifying the design through the stages while SSAR adds the set of guidelines and standards that will provide more detailed criteria for the development of the design. Tier 1 should be written to incorporate the most important and general aspects (top-level requirements) from the standards. The set of standards and criteria in DCD Tier 2 encompass the guidance for generating the plans that will be used in the I&C system design process throughout the lifecycle.

The certified design description and design development process continue for the lifetime of the plant. Any safety-related software that is changed or added after plant startup is required to either be developed using the certified design development process described in the computer Tier 1, or the licensee must submit a design process description (together with the design bases) that will produce software of the same or higher quality than the original certified design process, consistent with Tier 1. The licensee will be required to use the approved software change procedure (SCP) based upon the certified design development process for the operation stage of the lifecycle.

A. Diversity and Defense-In-Depth

Tier 1 should address the concern that software design faults or other initiating events common to redundant, multidivisional logic channels of I&C protection systems (or between different systems (safety and/or non-safety) could disable a significant portion of the plant's safety functions at the moment when these functions are needed to mitigate an accident, and addresses the diverse features that are provided for the primary automatic logic. SRP Section 7.1, 7.8 and BTP-HICB-19 describe the staff guidance for the review of the defense-in-depth and diversity provisions in the I&C system design.

B. Electromagnetic Interference (EMI)

Tier 1 should address the process to ensure that I&C equipment is able to function properly when subjected to an electromagnetic environment that is characteristic of the plant environment. An EMI compliance plan to confirm the level of immunity to

electrical noise should be included in the design, installation, and testing of I&C equipment. Refer to SRP Section 7.1 for EMI review criteria.

C. Setpoint Methodology

Tier 1 should address the process to ensure that setpoints for initiation of safety-related functions are determined, documented, installed, and maintained. The process (the instrument setpoint methodology) may establish a program for specifying requirements for documenting the bases for selection of trip setpoints, accounting for instrument loop inaccuracies, response testing, and maintenance or replacement of instrumentation. Reference SRP Chapter 7 BTP-HICB-12 for review criteria.

D. Equipment Qualification of I&C Components

Tier 1 should address the process to ensure that qualification of safety-related I&C equipment is able to complete its safety-related function under the environmental conditions that exist up to and including the time the equipment has finished performing that function. An equipment qualification program may be established that ensures qualification specifications consider conditions that exist during normal, abnormal, harsh and mild environments, and design-basis accident events in terms of their cumulative effect on equipment performance for the period up to the end of equipment life. Equipment qualification includes the qualification of isolation devices as described in SRP Chapter 7 BTP-HICB-11.

5. Software Development: In general, Tier 1 should discuss the following elements of software development.

A software QA (SQA) plan describes the software-specific activities that are to be performed and controlled in addition to the approved QA plan (in accordance with 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants") for the total ABWR design. The SQA plan establishes the criteria under which the other software development plans will be generated. The software management plan (SMP) establishes the organization and authority structure for the design, the procedures to be used, and the interrelationships between major activities. The software configuration management plan (CMP) provides the means to identify software products, control and implement changes, and record and report change implementation status. The software development plan (SDP) describes a development process, tools documentation, and products developed according to the software lifecycle. The verification and validation plan (V&VP) describes the method to ensure that the requirements of each phase or stage of the design process (lifecycle) are fully and accurately implemented into the next phase. Each safety-related software module should be verified by an organization that is independent of the organization that developed the software module. The software safety plan (SSP) describes the safety and hazards analyses that will be performed. The software operation and maintenance plan (SOMP) includes the procedures required to ensure that the software will be operated correctly and that the quality of the software is maintained. These plans may be combined into a

software management plan, a configuration management plan, and a verification and validation plan.

The ITAAC activities completed by the COL applicant will be audited by the NRC to verify conformance with the requirements at several stages during the digital control system design process or stage of the lifecycle. The documents which demonstrate satisfactory implementation of the ITAAC will be available for inspection during the NRC audit at the completion of each of the above stages. The stages or phases should be shown in Tier 1. The NRC audit and the COL applicant conformance review points are shown in Chapter 7 of the staff's safety evaluation report. These should correspond with the phases described by the applicant in Tier 1. The actual stages, including the conformance review and audit points, will be determined for each of the software products to be developed when design implementation is scheduled to begin.

At each stage, the design development must be verified by the COL applicant to be in accordance with the certified design process and the detailed design developed (through that stage) to be in conformance with the certified design. Upon completion of ITAAC activities for each stage, the COL applicant will certify to the NRC that the stage has been completed and the design and construction completed up through that stage is in compliance with the certified design. Although not required, the COL applicant should satisfactorily complete ITAAC activities at each stage prior to proceeding to the next stage of the design development process. Failure to successfully complete the ITAAC at a stage, as determined by the conformance review or the NRC audit, may require repeating an earlier stage ITAAC or changing the system design. The NRC staff will identify any open issues which require resolution for each stage of the ITAAC. Significant open issues which are not resolved could result in the NRC staff concluding that the ITAAC had not been satisfactorily completed.

The ITAAC should contain the following information:

- The specific design commitments to be verified by the ITAAC,
- The inspections, tests, and/or analyses to be performed, and
- The corresponding acceptance criteria which demonstrates that the design commitment has been met.

An example of one page of an ITAAC is provided in Figure 1 in this SRP section. The format of Tier 1/ITAAC is discussed further in Appendix A to this SRP section.

As a part of the submission for a design certification under Subpart B or a combined license under Subpart C of Part 52, the applicant must submit a proposed life cycle and all of the plans which are required in the first phase of that life cycle. The BTP on Software Process, BTP ICSB-14, and the BTP on Level of Detail, BTP ICSB-16, describe the HICB branch position on reviewing these planning documents. Since the planning commitments for the software development process are reviewed as part of the application, the software ITAAC needs to cover only those phases titled Requirements through Installation. See Figure 2 in this SRP section.

The software ITAAC should contain the commitments for each phase of the defined software development life cycle extracted from the planning documents, a method for verifying that each design commitment is met through inspection, test, or analysis, and an acceptance criterion for meeting the commitment. A set of acceptable commitments for each phase of the software life cycle is outlined in the BTP on Software Reviews, BTP ICSB-14, which also contains an acceptable method of verification and acceptable acceptance criteria for each of the commitments.

The commitments in the ITAAC should reflect in detail the elements, activities, and documentation required of the various phases of the life cycle as shown in Figure 1 and as detailed in the BTP on Software Reviews, BTP ICSB-14. Inspection should be the method for verifying the commitment and the acceptance criteria for each commitment should closely parallel the attributes listed in BTP ICSB-14. The acceptance criteria specified should be adequate to demonstrate that the software development activities committed to for each phase have been completed, and that these activities have produced the software attributes described in the BTP on Software Reviews, BTP ICSB-14.

The software development process outlined in this SRP section is such that as each phase is completed, more detail is added to the subsequent phases. For example, in the planning phase, a V&V plan is developed which commits the organization to a comprehensive software testing program. Then, during the design phase of the life cycle, detailed inspection and test plans are developed, including procedures and acceptance criteria. The detailed plans and procedures describe Tier 2 or Tier 2* attributes that represent commitments to be met. The inspections, tests, and the acceptance procedures which go with them should be adequate to assure that, if the tests are performed and the acceptance criteria are met, the system will perform according to its design (§52.47(a)(1)(vi) and §52.79(c)). The BTP on Software Reviews, BTP ICSB-14, describes software characteristics that should be demonstrated by the ITAAC or supporting Tier 2 verification activities.

Tier 2* Information

The material in DCD Tier 2 Chapter 7 provides design information and defines design processes that are acceptable for use in meeting the acceptance criteria in Tier 1. However, Tier 2 information may be changed by a COL applicant or licensee referencing the certified design in accordance with a "50.59-like" process that is specified in the design certification rule for the design. The staff bases its safety determinations on the design processes specified in SSAR. Therefore, for the evolutionary designs, the staff designated selected information in Tier 2 Chapter 7 that, if considered for a change, requires NRC approval prior to implementation. This information is known as Tier 2* information (see Appendix A for instructions on designating information in SSAR as Tier 2*). Similar information should be considered on a design-specific basis for all standard designs.

The areas in the design that are designated as Tier 2* shall be designated in the SER with the following statement: "Any changes to this commitment would require NRC approval prior to implementation." The rational for the selection of these items should be stated in the SER.

These items should typically be restricted to rapidly changing technology where it is inappropriate to "lock in" a design process for the lifetime of the design certification by placing the material in Tier 1, but would also be inappropriate to allow COL applicants or licensees to make unreviewed changes. Therefore, the items listed in Tier 2 should generally be the supporting material for the DAC.

The staff may allow some of the Tier 2* designation to expire after first full power operation of the facility, when the detailed design is complete and the facility performance characteristics are known from the initial test program. The NRC bears the final responsibility for designating which material in DCD Tier 2 is Tier 2*, and whether the designation will expire.

III. REVIEW PROCEDURES

1. Follow the general procedures for review of Tier 1 contained in the Review Procedures section of SRP Section 14.3. Ensure that the DCD is consistent with Appendix A to this SRP section. Review responsibilities may be consistent with those in Appendix B.

2. Ensure that all Tier 1 information is consistent with DCD Tier 2 information. Figures and diagrams should be reviewed to ensure that they accurately depict the functional arrangement and requirements of the systems. Reviewers should use the review checklists in Appendix C for review of systems as an aid in establishing consistent and comprehensive treatment of issues.

3. Ensure that the I&C systems are clearly described in Tier 1, including the key performance characteristics and safety functions of SSCs based on their safety significance.

4. The reviewer should ensure that appropriate guidance is provided to other branches such that I&C issues in Tier 1 are treated in a consistent manner among branches.

5. Ensure that the standard ITAAC entries in Appendix D related to I&C items are included in the appropriate systems of the standard design. In particular, the reviewer should ensure consistent application and treatment of the standard ITAAC entries for basic configuration ITAAC (environmental qualification aspects) and independence for electrical and I&C systems.

6. Reviewers should ensure that design features from the resolutions of selected technical and policy issues for the design are adequately addressed in Tier 1, based on safety significance. Ensure that the appropriate Commission guidance, requirements, bases, and resolutions for these items are documented clearly in the SER.

7. Reviewers should confirm the ITAAC and DAC covers all software development activities from the completion of process planning through the completion of system installation and confirm the ITAAC includes each commitment made in the software development planning documents. Reviewers should also confirm that the ITAAC and DAC defines acceptable methods and acceptance criteria for confirming each commitment is met. Supporting information should be in the appropriate sections of Tier

2. Ensure that the applicable material in Tier 2 is designated as Tier 2* with appropriate expiration dates. Ensure that the Tier 2* material is identified in the SER, and the bases for the Tier 2* designation.

8. Reviewers should confirm via a sequence of audits that the ITAAC is appropriately implemented by applicants, and that it demonstrates the software process is developing quality software as described in BTP ICSB-14. NUREG/CR-Task 9 provides detailed information that may be used in auditing the performance of software ITAAC.

IV. EVALUATION FINDINGS

The reviewer verifies that sufficient information has been provided to satisfy the requirements of this SRP section, and concludes that Tier 1 is acceptable. The findings should be similar to those in the Evaluation Findings section of SRP Section 14.3.

If the applicant has provided DAC for various aspects of the standard design, then the reviewer should provide a separate evaluation similar to the above for that material.

V. IMPLEMENTATION

The following is intended to provide guidance to applicants and licensees regarding the NRC staff's plans for using this SRP section.

This SRP section will be used by the staff when performing safety evaluations of design certification and combined license applications submitted by applicants pursuant to 10 CFR 52. Except in those cases in which the applicant proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the method described herein will be used by the staff in its evaluation of conformance with Commission regulations.

The provisions of this SRP section apply to reviews of applications docketed six months or more after the date of issuance of this SRP section.

VI. REFERENCES

1. 10 CFR Part 50, "Code of Federal Regulations - Energy - Domestic licensing of production and utilization facilities."

2. 10 CFR Part 52, "Code of Federal Regulations - Energy - Early site permits; standard design certifications; and combined licenses for nuclear power plants."

3. SECY-91-178, "Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for Design Certifications and Combined Licenses."

4. SECY-91-210, "Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Requirements for Design Review and Issuance of a Final Design Approval (FDA)."

5. SECY-92-053, "Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Reviews."

6. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems."

7. NUREG/CR-Task 9, "Assessing Safety-Critical Software in Nuclear Power Plants."

8. NUREG-1503, "Final Safety Evaluation Report Related to the Certification of the Advanced Boiling Water Reactor", Volumes 1 and 2, July 1994.

9. NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design," Volumes 1 and 2, August 1994.

The following IEEE standards are referenced in NUREG/CR-6101 and are included here for completeness.

10. IEEE Std 730.1-1989, "Software Quality Assurance Plans."

11. IEEE Std 828-1984, "Software Configuration Management Plans."

12. IEEE Std 830-1985, "Software Requirements Specifications."

13. IEEE Std 1012-1986, "Software Verification and Validation Plans."

14. IEEE Std 1058.1-1987, "Standard for Software Project Management Plans."

15. IEEE Std P-1228, "Standard for Software Safety Plans."

16. IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

Inspections, Tests, Analyses and Acceptance Criteria		
Design Commitment	**Inspections, Tests, or Analyses**	**Acceptance Criteria**
7. A quality assurance program encompassing software is employed as a controlled process for software development, hardware integration, and final product and system testing.	7. The program for quality assurance that encompasses software shall be reviewed.	7. A quality assurance program is in place that defines controlled processes for software development, hardware integration, and final product and system testing. As a minimum, the program requires a Software Management Plan, Configuration Management Plan and Verification and Validation Plan as described in the following items.
8. A Software Management Plan (SMP) shall be instituted which establishes that software for embedded control hardware shall be developed, designed, evaluated, and documented per a design development process. The software safety issues shall be defined at each life-cycle phase of the software development. For each life-cycle phase, the SMP shall define the current state of that design phase and the input for the next design phase.	8. The Software Management Plan shall be reviewed.	8. The Software Management Plan shall define: a. The organization and responsibilities for development of the software design; the procedures to be used in the software development; the interrelationships between software design activities; and the methods for conducting software safety analyses. b. That the software safety analyses to be conducted for safety-related software applications shall: (1) Identify software requirements having safety-related implications. (2) Document the identified safety-critical software requirements in the software requirements specification for the design.

Figure 1. Example Instrumentation and Control ITAAC (excerpt)

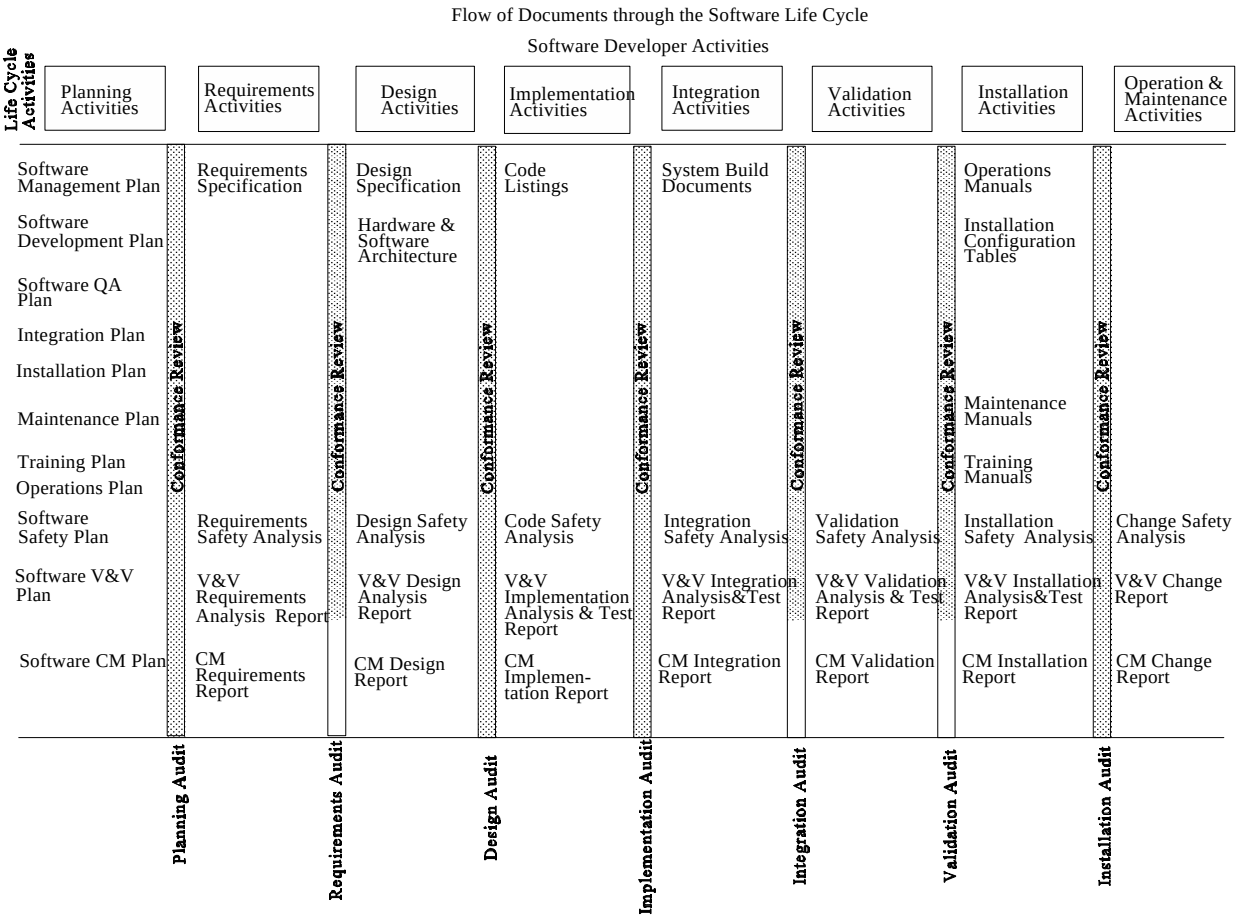

Figure 2. Flow of Documents through the Software Life Cycle

[This Page Intentionally Left Blank]

SRP Draft Section 14.3.51
Attachment A - Proposed Changes in Order of Occurrence

Item numbers in the following table correspond to superscript numbers in the redline/strikeout copy of the draft SRP section.

Item	Source	Description
1.	**Integrated Impact 1538**	The scope and content of this proposed SRP section is derived from the requirements of 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," as well as the guidance in staff SECY papers related to design certification and combined license reviews, and the staff positions established in the Final Safety Evaluation Reports (FSERs) for the evolutionary reactor designs.SRP Section 14.3.5 provides guidance specific to the review of instrumentation and controls design information and related inspections, tests, analyses, and acceptance criteria (ITAAC) provided in applications submitted in accordance with the requirements of 10 CFR 52.

[This Page Intentionally Left Blank]

Integrated Impact No.	Issue	SRP Subsections Affected
1538	Develop Acceptance Criteria and Review Procedures for review of Certified Design Material (CDM) including associated inspections, tests, analyses and acceptance criteria (ITAAC) for instrumentation and controls.	All